Homeland Security

May 2010

ICSJWG Newsletter

## ICSJWG 2010 Fall Conference

The ICSJWG 2010 Fall Conference will be held in Seattle, WA, at the Renaissance Seattle Marriott Hotel from October 25-28. The first day of the conference will be dedicated to subgroup working meetings followed by two days of subgroup and speaker presentations. There will be a one day introductory controls systems security training after the conference.

More information is available at:

http://www.us-cert.gov/control_systems/icsjwg/conference.html

### About the ICSJWG

***The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.***

***For more information, visit http://www.us-cert.gov/control_systems/icsjwg/***

## ICSJWG Subgroups

Several of the ICSJWG Subgroups met in May. Below is an update on the progress of these subgroups.

**Information Sharing Subgroup**
**Co-Chairs:** George Bamford and Nathan Faith

The Information Sharing Subgroup did not meet in May, but will resume meeting after the Homeland Security Information Network (HSIN) tool has been launched.

**International Subgroup**
**Co-Chairs:** Seán McGurk and Michael Assante

The International Subgroup did not meet in May, but will resume meeting after HSIN has been launched.

**Research and Development Subgroup**
**Co-Chairs:** Dr. Douglas Maughan (Douglas.Maughan@dhs.gov) and David L Norton (DNORTO1@entergy.com).

The focus of the meeting was on objective #1 in their charter, which is to identify existing and planned R&D needs and priorities as they relate to ICS. The group agreed that they need input from owners and operators as well as further discussions with vendors. Completing this objective should help to drive the R&D subgroup closer to its larger goals. The R&D Subgroup is actively seeking increased participation from industry stakeholders.

**Roadmap to Secure Industrial Control Systems**
**Co-Chairs:** Perry Pederson (perry.pederson@nrc.gov) and Tim Roxey (Tim.Roxey@nerc.net).

The Roadmap Subgroup continues to make progress on the draft *Cross-Sector Roadmap to Secure Control Systems*. The team is now reviewing a newly added section to the document pertaining to metrics to measure current status and progress. The final document is planned to be published in 2011.

The group formalized a monthly meeting schedule. The group will meet the fourth Thursday of each month from 11am-12pm EST.

**Vendor Subgroup**
**Co-Chairs:** Rick Lichtenfels (cssp@dhs.gov) and Eric Cosman (ECCosman@dow.com).

The focus of the meeting was the subgroup charter. The discussion emphasized a fresh look at the challenges that the vendors, owners, and operators face and how the subgroup can help. The group also reviewed its objectives and goals to determine whether they were still relevant and if so, the approaches to achieving them.

The group formalized a monthly meeting schedule. The group will meet the fourth Monday of each month from 2-3pm EST.

**Workforce Development Subgroup**
**Co-Chairs:** Ben Wible (wibleb@ndu.edu), Dr. John Saunders (saunders@ndu.edu), and Marcus Sachs (marcus.sachs@verizon.com).

The co-chairs are currently working on a white paper to derive recommendations from a gap analysis of industrial controls systems security curricula. It will be published for the Fall ICSJWG conference.

If you would like to contribute to the group, please email icsjwg@dhs.gov.

The group formalized a monthly meeting schedule. The group will meet the third Thursday of each month from 1-2pm EST.

## *Homeland Security Information Network (HSIN)*

The ICSJWG HSIN portal is still under development and will be available in a couple of weeks.

- If you need an HSIN account:
    - **Federal Employees:** Any federal employee who would like an HSIN ICSJWG account must be vetted and granted access through the HSIN-CS/ICSJWG portal administrators: Sunny Browarny (NCSD) and Adam Zoller (I&A) at ICSJWG@dhs.gov.
    - **Private Sector Partners:** Any private sector partner who would like access to HSIN must be vetted through their respective sector administrator (i.e. electrical sector partners obtain accounts through the electric sector administrator).

- If you already have an HSIN account, please provide your name, HSIN user name, ICSJWG subgroup affiliation, and critical infrastructure sector, to ICSJWG@dhs.gov so we can provide you with access to the HSIN ICSJWG portal once it becomes available.

## *Participation is Key!*

Your participation and input is **critical** to the success of these subgroups and to the overall mission of ICSJWG to coordinate cybersecurity efforts to secure ICS across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

## *Advanced Training Events Scheduled for 2010*

This event will provide intensive hands-on training on protecting and securing control systems from cyber attacks, including a very realistic Red Team / Blue Team exercise that will be conducted within an actual control systems environment. It will also provide an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.
The following advance training events have been scheduled for the remainder of 2010:

- June 21-25, 2010 – International
- July 19-23 – Federal Partners
- Sept. 13-17 – US Asset Owners and Vendors

Additional offerings are being planned and will be announced once dates are finalized. The training is held at the Control Systems Analysis Center located in Idaho Falls, Idaho, and provides an intensive, hands-on environment. Students gain experience protecting and securing industrial control systems from cyber attacks, including a Red Team /Blue Team exercise that is conducted within an actual control systems environment.

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant. More information, including registration and future offerings is available at: http://www.us-cert.gov/control_systems/

## *Conference Events Scheduled for 2010*

The following is a listing of upcoming conferences and other events that the Control Systems Security Program (CSSP) is supporting and may be of interest to individuals involved in control systems security.

- June 13-18, 2010 - **22nd Annual FIRST Conference**
  - http://conference.first.org/
- June 14-16, 2010 - **Smart Electricity World USA 2010**
  - http://www.terrapinn.com/2010/smartusa/
- June 20-24, 2010 - **American Water Works Association ACE 10 Conference**
  - http://www.awwa.org/

- June 21-23, 2010 - **Critical Infrastructure Security Summit**
  - http://www.criticalinfrastructuresummit.com
- July 27-29, 2010 - **HydroVision International**
  - http://www.hydroevent.com/index.html

Additional conferences will be announced once CSSP participation is finalized.

## *Contact Information*

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at https://forms.us-cert.gov/report/.

Other important contact information:
Web Site Address: http://www.us-cert.gov/control_systems/
ICS-CERT Email: ics-cert@dhs.gov
Phone: 1-877-776-7585
CSSP Email: cssp@dhs.gov